(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2001 (10.05.2001)

PCT

(10) International Publication Number
WO 01/33889 A1

(51) International Patent Classification[7]: H04Q 7/38, H04L 29/06

(21) International Application Number: PCT/IB00/01586

(22) International Filing Date:
1 November 2000 (01.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/162,987 1 November 1999 (01.11.1999) US
60/184,793 24 February 2000 (24.02.2000) US

(71) Applicant: WHITE. CELL, INC. [IL/IL]; Amal Street 11, Afeq Industrial Park, 48092 Rosh-HaAyin (IL).

(71) Applicant and
(72) Inventor: AMITAI-ORENY, Dganit [IL/IL]; Yaari Street 4, 69371 Tel-Aviv (IL).

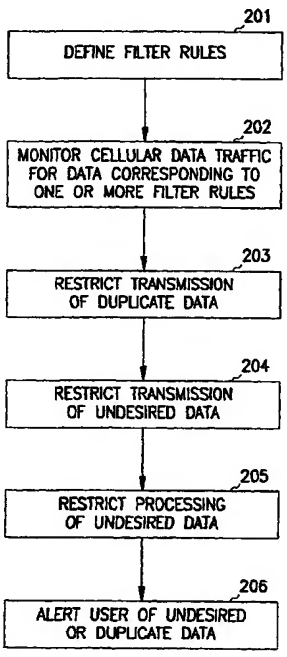
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: CELLULAR DATA SYSTEM SECURITY METHOD AND APPARATUS



(57) Abstract: The present invention provides a system providing security in a cellular data system than can monitor and restrict undesired or malicious data. In one embodiment, the system uses one or more defined filter rules to identify data that is undesired or duplicate data, monitors cellular data traffic for data corresponding to one or more of the filter rules, and restricts transmission or use of cellular data found to correspond to one or more of the filter rules.

WO 01/33889 A1

Cellular Data System Security Method and Apparatus

Field of the Invention

The invention relates generally to security in cellular data systems, and more specifically to providing a security method and apparatus to protect digital data and equipment in cellular data networks such as those providing cellular Internet access.

Claim of Priority

This application is related to and claims priority from pending provisional application 60/162,987, "Controlled & Safe Data Services for Real Time Devices", filed 11/01/99, and application 60/184,793, "Data System Security Method and Apparatus", filed 2/24/2000.

Background of the Invention

Cellular telephones and wireless computerized cellular devices are rapidly evolving to incorporate capabilities traditionally found only on large networked computers, and are frequently used to access the Internet or other networks. Current generations of such devices have limited but expanding capabilities, and often incorporate versions of web browsers, e-mail clients, and other common Internet data retrieval tools.

It is anticipated that as the capabilities of these cellular data devices grow, they will become favored for some types of Internet use that are well-suited to mobile or time-sensitive applications, such as receiving e-mail or other urgent messages, trading stocks, looking up data such as maps or movie times and listings while away from home, and other such uses. Still other uses are expected to evolve as this technology develops, possibly including new e-commerce, multimedia, or additional data retrieval and messaging applications.

A number of competing protocols such as WAP (Wireless Application Protocol) and others have been developed to facilitate exchange of data between cellular networks and mobile cellular equipment, most of which are used to facilitate Internet access via the mobile equipment and the cellular network system. These cellular network systems typically both receive data from the Internet or another information source and convert it to data encoded with the

appropriate protocol for sending to the mobile cellular equipment, and receive data from the mobile cellular equipment and convert it for sending over the Internet or other destination. Therefore, mobile cellular equipment can communicate via a supported protocol through the cellular network system to the Internet or other information source, using services provided by the cellular network system.

But, it is also anticipated that as cellular mobile equipment with such capability becomes more common, so too will the plague of viruses, spam, trojan horse application, flood attacks, and other malicious data currently propagated over networks such as the Internet. In the Internet context, firewalls and virus scanning software have evolved to challenge many such types of malicious data. Unfortunately, simple virus scanners or firewalls are not easily or effectively adaptable to a cellular network or to mobile cellular equipment, and so the threat of malicious or undesired data is largely yet unsolved. Further, some threats such as flooding are not addressable using other methods such as encryption, and other solutions similarly often fail to address a wide variety of likely potential threats.

Current cellular data security systems typically provide only encryption or authentication, and the security provided by these systems has recently been questioned. Even if secure, hostile or undesired data from the Internet or another source may be unknowingly retrieved despite implementation of these systems without any way of detecting its nature until the data has done harm. Security problems therefore still exist in a variety of environments and applications, and mobile cellular equipment largely remains susceptible to attack from hackers, viruses, and other hostile or undesired data.

What is needed is a system providing security in a cellular data system that can monitor and restrict undesired or malicious data.

Summary of the Invention

The present invention provides a system providing security in a cellular data system that can monitor and restrict undesired or malicious data. In one embodiment, the system uses one or more defined filter rules to identify data that is undesired or duplicate data, monitors cellular data traffic for data

corresponding to one or more of the filter rules, and restricts transmission or use of cellular data found to correspond to one or more of the filter rules.

Brief Description of the Figures

Figure 1 shows a cellular data network connected to an external network with mobile cellular equipment, as may be used to practice an embodiment of the present invention.

Figure 2 is a diagram illustrating elements of one example embodiment of the present invention.

Figure 3 is a diagram illustrating elements of an embodiment of the present invention incorporating message delivery tracking capability.

Figure 4 is a diagram illustrating an embodiment of the present invention incorporating operation supporting filtering data in a non-protocol specific format.

Detailed Description

In the following detailed description of sample embodiments of the invention, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific sample embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical, and other changes may be made without departing from the spirit or scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the invention is defined only by the appended claims.

The present invention provides a system providing security in a cellular data system that can monitor and restrict undesired or malicious data. The system provides in various embodiments use of one or more defined filter rules to identify data that is undesired or duplicate data. The system then monitors cellular data traffic for data corresponding to one or more of the filter rules, and restricts in various embodiments of the invention transmission or use of cellular data found to correspond to one or more of the filter rules.

Figure 1 is a block diagram that illustrates one possible structure into which a system to practice the present invention may be incorporated. An

external network 101 such as the Internet or an external telephone network is connected via a connection 103 to a local cellular data network 102 that is operated by a cellular service provider. Each cell within the service provider's service region employs one or more antennas 104 to facilitate wireless communication with subscriber's mobile cellular equipment 105.

In operation, a system incorporating the present invention may be implemented within the external network 101 before connection via 103 to the local cellular data network 102, within the cellular data network 102, or within the mobile cellular equipment 105. In practice, the invention may therefore be incorporated anywhere within the data chain between the mobile cellular equipment and other originators of cellular data, including within the cellular data networks, mobile cellular equipment, or other equipment of other network service providers or cellular service providers.

One exemplary embodiment of the invention presented in Figure 2 first requires definition of filter rules at 201. The filter rules are defined to serve as a reference with which to determine what cellular data traffic will be deemed undesired or duplicate data. The filter rules may in various embodiments of the invention be defined by mobile cellular equipment users, by cellular service providers, by an automated cellular data monitoring system, by a filter rule subscription or distribution service, or by any other method of creating filter rules usable to identify undesired or duplicate data.

The filter rules may be implemented in any way that facilitates examination of cellular data traffic for corresponding data, including in various embodiments of the invention implementation via state machines, defined key fields corresponding to fields in the cellular data stream, location-specific restrictions on content or quantity of information, or any other suitable method. The filter rules will in various embodiments be defined to enable identification of duplicate or undesired data, and may include rules that use the location of mobile cellular equipment as a parameter.

The filter rules defined at 201 may in some embodiments of the invention be automatically propagated through a network, including within or between cellular data networks, mobile cellular equipment, and external network equipment. In other embodiments, the filter rules may be optionally received

from a distribution source, or received automatically but requiring user approval before utilization.

The filter rules will in various embodiments of the invention be configured to define duplicate key fields in cellular data, such that these key fields can be used to monitor cellular data traffic at 202 to determine whether cellular data is duplicate data. In one specific embodiment of the invention, this is accomplished by building a table comprising a table entry for each address detected in monitoring cellular data. Each table entry then records both the time of the last detected cellular data corresponding to the address, and a counter that counts the duplicate cellular data corresponding to the address over a period of time. Such a system can monitor both source and destination addresses, thereby preventing both floods to a single destination from multiple sources and floods or spam from a single source to multiple other destinations.

Duplicate data includes not only data that is determined to have the same address as other data, but in other embodiments includes having the same data in one or more other fields. For example, data from a single network domain that contains the same data as other cellular data traffic may be deemed duplicate despite being from a different address. Many other key fields or combinations of key fields may be used in different embodiments of the invention to determine duplication of data, and are within the scope of the invention.

Data determined to be duplicate data is then restricted from transmission at 203, and a user is optionally alerted in some embodiments of the invention at 206. The user may be a mobile equipment user, a cellular data network equipment user or cellular service provider, or be an external network user. The user will in some further embodiments be able to inspect and discard or forward the data, log the data, create new filter rules in response to the data, or take other appropriate action in response to the alert.

Restricting transmission of the data at 203 in further embodiments comprises delaying transmission of duplicate data that exceeds a predetermined allowable amount of duplicate cellular data per period of time. Restricting transmission in various other embodiments may comprise storing the duplicate data for later evaluation, reporting of the duplicate data to a cellular service

provider for transmission approval, possible approval and logging of duplicate data to enable billing for authorized mass advertising, or other means of restriction.

The filter rules defined at 201 may also address other types of data that are unwanted, such that the filter rules are used at 202 in monitoring cellular data traffic for the udesired data corresponding to the one or more filter rules. This undesired data can be restricted from further transmission at 204 such as when detected in a cellular data network of a cellular service provider, or can be restricted from processing at 205 such as when detected in mobile cellular equipment.

One or more filter rules corresponding to the undesired data type have been defined at 201, and again may address a variety of undesired data types using any variety of rule parameters. For example, the filter rules may be address-specific, user-configurable, or simply mass distributed rules directed toward known threats. The undesired data types include in various embodiments but are not limited to known viruses, trojan horses, spam, data originating from addresses or network regions known or suspected to be associated with hacking activity, undesired advertising or personal addresses, data of a size larger than is desired for automatic downloading, or other undesirable data.

In some embodiments of the invention, the system implementing the monitoring function at 202 is further operable to track messages delivered to cellular mobile equipment. Figure 3 is a flowchart that illustrates integration of tracking functions into a system that monitors cellular data traffic as shown at 202 and at 301. Messages delivered to mobile cellular equipment are tracked at 302, and the tracking data is used to create call log reports from tracked messages at 303. The tracking data is also used in a further embodiment to create billing reports or to create billing data at 304. The billing can be based on tracking data comprising the number of messages or other data elements delivered, the bandwidth consumed in receiving data, the speed or other level of service with which data is retrieved, or other such factors.

The mobile cellular equipment address or other identifying characteristics may be filtered via the filter rules to prevent propagation of selected mobile cellular equipment identifiers or cell identifiers from propagating through a

cellular or external network, preventing transmission of data that could be used to locate the cellular mobile equipment. This restriction of cellular mobile equipment registration data propagation is implemented in selected embodiments of the invention to protect user privacy, so that the registration or address data cannot be intercepted and used to determine in which cell a particular mobile cellular equipment user is located.

The inventive system described herein may be implemented within a system utilizing multiple data streams that are encoded with multiple cellular data protocols, and desirably will have monitoring capability to monitor cellular data traffic in any protocol supported within the network. Examples of such protocols include WAP, GPRS, SMS, CIMD, NIP, OIS and TCP/IP protocols such as SMPP and UCP. Other protocols exist and are likely to be developed, and the protocols here are listed as examples only. In such systems, it is desirable to monitor cellular data traffic as shown at 202 in a manner such as is illustrated in Figure 4. At 401, filter rules are defined in a non-format specific format. Cellular data is intercepted within the system at 402, and the intercepted data is parsed into a non-protocol specific format at 403. The parsed data is stored in a data structure in non-protocol specific format at 404, and the data is then compared against the filter rules at 405. Elements 402 through 405 largely correspond to monitoring cellular data at 202 of Figure 2, and comprise yet another possible embodiment of the invention as described in conjunction with Figure 4.

The present invention may also be implemented in some embodiments within mobile cellular equipment 105. Various embodiments will employ an event monitor operating in hardware or software within mobile cellular equipment that is operable to limit the function of software that executes on the mobile cellular equipment. The restrictions to software function include in some embodiments limiting the ability of executing software to erase or modify data stored on the mobile cellular equipment. Embodiments of the invention implemented within mobile cellular equipment will likely be particularly well-suited for implementation of user-configurable filter rules, so that a user can control the degree of security and functionality of his own mobile cellular equipment. But, filter rules may still in various embodiments be received from a

distribution server or via other methods, such as to receive automatic virus or trojan horse filter rule updates.

A Subscriber Identity Module (SIM) is employed in some moblie cellular equipment such as is shown at 105, and filter rules may specifically be employed to prevent unauthorized modification of data contained in the SIM. The monitoring and restricting functions of the present invention may be employed in various embodiments within the SIM, in an interface between the SIM and the mobile cellular equipment, or within the mobile cellular equipment.

In cellular mobile equipment as well as in other embodiments of the invention, various actions may be taken once duplicate or undesired data is identified. In addition to restricting transmission or processing of the data, some embodiments of the invention will incorporate prompting a user to determine appropriate action. For example, a cellular mobile equipment user may be given the option to halt execution of suspect code, or may select to execute the code despite the warning. In other embodiments, a cellular data network or other network operator may receive notification of undesired or duplicate data, and therefore may use the data to alert people of the threat or take actions to eliminate the undesired or duplicate data. A help desk may also be alerted in some embodiments of the invention, and may contact appropriate cellular equipment users to assist them in dealing with the undesired or duplicate data.

Implementation of the invention in some embodiments will require communication of cellular data traffic over an external network via a protocol such as TCP/IP that may not include certain address or identification information normally communicated within a cellular data network such as 102. In such embodiments, dynamic IP translation will desirably be implemented to map a certain address, phone number, or other location identifier to a TCP/IP address or other external network address, to facilitate tracking of this data and filtering based on this data. For example, a mobile cellular equipment user may configure his equipment to reject cellular data traffic from a specific telephone number. If this undesired data originates remotely from the local cellular data network and must travel to the local network via an external network using TCP/IP or another protocol that does not directly preserve and transmit the originator's phone number, dynamic IP or address translation will be needed to

preserve and identify the originator's phone number. By associating the originator's phone number with the address used in the external TCP/IP network, the phone number can be reassociated with the cellular data with the specific IP address on reaching the local cellular data network, and so may be used there for filtering.

The present invention may be implemented in hardware, in software, or in any other manner consistent with the appended claims. It is anticipated that the examples given herein are descriptive of currently desirable applications of the invention, but it is also anticipated that many other example embodiments of the present invention will become apparent only as mobile cellular equipment and its use for data access evolve.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the invention. It is intended that this invention be limited only by the claims, and the full scope of equivalents thereof.

Claims

1. A method of providing security in a cellular data system, comprising

defining one or more filter rules, at least one of the filter rules to be used to identify cellular data that is duplicate data;

monitoring cellular data traffic for data corresponding to one or more of the filter rules; and

restricting transmission of the cellular data traffic corresponding to the one or more filter rules.

2. The method of claim 1, wherein the at least one filter rule is used to identify duplicate key fields in the cellular data, the key fields comprising a source address of an originator of the cellular data.

3. The method of claim 1, further comprising building a table comprising a table entry for each address detected in the cellular data, each table entry comprising:

a timestamp of the last cellular data sent to or from the address corresponding to the table entry; and

a counter that counts duplicate cellular data corresponding to the table entry per period of time.

4. The method of claim 3, wherein each table entry comprises key fields to be used to identify the cellular data as duplicate.

5. The method of claim 1, wherein restricting transmission of the cellular data traffic corresponding to the one or more filter rules comprises blocking duplicate cellular data that exceeds a predetermined allowable amount of duplicate cellular data per period of time from transmission.

6. The method of claim 1, wherein restricting transmission of the cellular data traffic corresponding to the one or more filter rules comprises delaying transmission of duplicate cellular data that exceeds a predetermined allowable amount of duplicate cellular data per period of time.

7. A method of providing security in a cellular data system, comprising

defining one or more filter rules, each filter rule corresponding to an undesired data type;

monitoring cellular data traffic for data corresponding to one or more of the filter rules in a networked computerized system comprising part of a cellular data network; and

restricting transmission of the cellular data traffic corresponding to the one or more filter rules in the networked computer.

8. The method of claim 7, wherein the networked computerized system further tracks messages delivered through a cellular data network to cellular mobile equipment.

9. The method of claim 8, further comprising creating billing reports from the tracked messages.

10. The method of claim 8, further comprising creating call log reports from the tracked messages.

11. The method of claim 7, wherein the networked computerized system resides between a computer data network and a cellular data network.

12. The method of claim 7, wherein the networked computerized system resides within a cellular data network.

13. The method of claim 7, wherein the networked computerized system marks data that has been monitored via the filter rules in the networked computer to indicate monitoring.

14. The method of claim 7, wherein the cellular data traffic comprises multiple data streams encoded via multiple cellular data protocols.

15. The method of claim 7, wherein monitoring cellular data traffic comprises:

intercepting cellular data;

parsing the intercepted data to a data structure that is non-protocol specific; and

comparing the intercepted data in the data structure against filter rules.

16. The method of claim 7, wherein the cellular data comprises mobile equipment cell registration data that is restricted via filter rules to prevent network transmission of the location of cellular mobile equipment.

17. A method of providing security in a cellular data system, comprising

defining one or more filter rules, each filter rule corresponding to an undesired data type;

monitoring cellular data traffic for data corresponding to one or more of the filter rules in cellular mobile equipment; and

restricting processing of the cellular data traffic corresponding to the one or more filter rules in the cellular mobile equipment.

18. The method of claim 17, wherein the monitoring and restricting occurs in an event monitor, the event monitor operable to limit the function of software executing on the cellular mobile equipment by use of the filter rules.

19. The method of claim 18, wherein limiting the function of software executing on the mobile equipment comprises limiting the ability of executing software to erase or modify data stored on the cellular mobile equipment.

20. The method of claim 17, wherein the filter rules comprise rules that can be configured by a user via operation of the cellular mobile equipment.

21. The method of claim 17, wherein the filter rules comprise rules that are distributed via a server.

22. The method of claim 17, wherein monitoring cellular data traffic comprises:

intercepting cellular data;

parsing the intercepted data to a data structure that is non-protocol specific; and

comparing the intercepted data in the data structure against filter rules.

23. The method of claim 17, wherein restricting processing of data that corresponds to one or more filter rules comprises temporarily halting processing of the data and prompting a cellular system user to determine what action to take.

24. The method of claim 17, wherein restricting processing of data that corresponds to one or more filter rules comprises temporarily halting processing of the data and alerting a user.

25. The method of claim 16, wherein the monitoring and restricting processing of data that corresponds to one or more filter rules occurs in an interface that resides between a subscriber identity module (SIM) and cellular mobile equipment.

26. The method of claim 25, wherein the one or more filter rules restrict modification of data contained in the subscriber identity module (SIM).

27. A computerized information management system, the system operable to:

store one or more filter rules, at least one of the filter rules to be used to identify cellular data that is duplicate data;

monitor cellular data traffic for data corresponding to one or more of the filter rules; and

restrict transmission of the cellular data traffic corresponding to the one or more filter rules.

28. The computerized information management system of claim 27, wherein the at least one filter rule is usable to identify duplicate key fields in the cellular data, the key fields comprising a source address of an originator of the cellular data.

29. The computerized information management system of claim 27, further comprising a table that comprises a table entry for each address detected in the cellular data, each table entry comprising:

a timestamp of the last cellular data sent to or from the address corresponding to the table entry; and

a counter that counts duplicate cellular data corresponding to the table entry per period of time.

30. The computerized information management system of claim 29, wherein each table entry further comprises key fields to be used to identify the cellular data as duplicate.

31. The computerized information management system of claim 27, wherein restricting transmission of the cellular data traffic corresponding to the one or more filter rules comprises blocking duplicate cellular data that exceeds a predetermined allowable amount of duplicate cellular data per period of time from transmission.

32. The computerized information management system of claim 27, wherein restricting transmission of the cellular data traffic corresponding to the one or more filter rules comprises delaying transmission of duplicate cellular data that exceeds a predetermined allowable amount of duplicate cellular data per period of time.

33. A networked computerized information management system comprising part of a cellular data network, the system operable to:

define one or more filter rules, each filter rule corresponding to an undesired data type;

monitor cellular data traffic for data corresponding to one or more of the filter rules; and

restrict transmission of the cellular data traffic corresponding to the one or more filter rules.

34. The computerized information management system of claim 33, wherein the system is further operable to track messages delivered through a cellular data network to cellular mobile equipment.

35. The computerized information management system of claim 34, wherein the system is further operable to create billing reports from the tracked message data.

36. The computerized information management system of claim 34, wherein the system is further operable to create call log reports from the tracked message data.

37. The computerized information management system of claim 33, wherein the system resides between a computer data network and a cellular data network.

38. The computerized information management system of claim 33, wherein the system resides within a cellular data network.

39. The computerized information management system of claim 33, wherein the system is further operable to mark data that has been monitored via the filter rules in the system to indicate monitoring.

40. The computerized information management system of claim 33, wherein the cellular data traffic comprises multiple data streams encoded via multiple cellular data protocols.

41. The computerized information management system of claim 33, wherein monitoring cellular data traffic comprises:

intercepting cellular data;

parsing the intercepted data to a data structure that is non-protocol specific; and

comparing the intercepted data in the data structure against filter rules.

42. The computerized information management system of claim 33, wherein the cellular data comprises mobile equipment cell registration data that is restricted via filter rules to prevent network transmission of the location of cellular mobile equipment.

43. Cellular mobile equipment, the cellular mobile equipment operable to:

store one or more filter rules, each filter rule corresponding to an undesired data type;

monitor cellular data traffic for data corresponding to one or more of the filter rules; and

restrict processing of the cellular data traffic corresponding to the one or more filter rules.

44. The cellular mobile equipment of claim 43, wherein the monitoring and restricting occurs in an event monitor module within the cellular mobile equipment, the event monitor operable to limit the function of software executing on the cellular mobile equipment by use of the filter rules.

45. The cellular mobile equipment of claim 44, wherein limiting the function of software executing on the mobile equipment comprises limiting the ability of executing software to erase or modify data stored on the cellular mobile equipment.

46. The cellular mobile equipment of claim 43, wherein the filter rules comprise rules that can be configured by a user via operation of the cellular mobile equipment.

47. The cellular mobile equipment of claim 43, wherein the filter rules comprise rules that are distributed via a server.

48. The method of claim 43, wherein monitoring cellular data traffic comprises:

intercepting cellular data;

parsing the intercepted data to a data structure that is non-protocol specific; and

comparing the intercepted data in the data structure against filter rules.

49. The cellular mobile equipment of claim 43, wherein restricting processing of data that corresponds to one or more filter rules comprises temporarily halting processing of the data and prompting a cellular system user to determine what action to take.

50. The cellular mobile equipment of claim 43, wherein restricting processing of data that corresponds to one or more filter rules comprises temporarily halting processing of the data and alerting a user.

51. The cellular mobile equipment of claim 43, wherein the monitoring cellular data traffic and restricting processing of data that corresponds to one or more filter rules occurs in an interface comprising a part of the cellular mobile equipment that resides between a subscriber identity module (SIM) and cellular mobile equipment.

52. The cellular mobile equipment of claim 51, wherein the one or more filter rules restrict modification of data contained in the subscriber identity module (SIM).

53. A cellular mobile equipment hardware interface, the interface insertable between a subscriber identity module (SIM) and cellular mobile equipment and operable when so inserted to:

monitor cellular data traffic for data corresponding to one or more filter rules; and

restrict processing of the cellular data traffic corresponding to the one or more filter rules.

54. A machine-readable medium with instructions stored thereon, the instructions when executed operable to cause a computerized system to:

store one or more filter rules, at least one of the filter rules to be used to identify cellular data that is duplicate data;

monitor cellular data traffic for data corresponding to one or more of the filter rules; and

restrict transmission of the cellular data traffic corresponding to the one or more filter rules.

55. The method of claim 54, wherein the at least one filter rule is used to identify duplicate key fields in the cellular data, the key fields comprising a source address of an originator of the cellular data.

56. The machine-readable medium of claim 54, the instructions further operable when executed to cause the computerized system to build a table comprising a table entry for each address detected in the cellular data, each table entry comprising:

a timestamp of the last cellular data sent to or from the destination address corresponding to the table entry; and

a counter that counts duplicate cellular data corresponding to the table entry per period of time.

57. The machine-readable medium of claim 56, wherein each table entry comprises key fields to be used to identify the cellular data as duplicate.

58. The machine-readable medium of claim 54, wherein restricting transmission of the cellular data traffic corresponding to the one or more filter rules comprises blocking duplicate cellular data that exceeds a predetermined allowable amount of duplicate cellular data per period of time from transmission.

59. The machine-readable medium of claim 54, wherein restricting transmission of the cellular data traffic corresponding to the one or more filter rules comprises

delaying transmission of duplicate cellular data that exceeds a predetermined allowable amount of duplicate cellular data per period of time.

60. A machine-readable medium with instructions stored thereon, the instructions when executed operable to cause a networked computerized system comprising part of a cellular data network to:

store one or more filter rules, each filter rule corresponding to an undesired data type;

monitor cellular data traffic for data corresponding to one or more of the filter rules in a networked computer comprising part of a cellular data network; and

restrict transmission of the cellular data traffic corresponding to the one or more filter rules in the networked computer.

61. The machine-readable medium of claim 60, the instructions when executed further operable to track messages delivered through a cellular data network to cellular mobile equipment.

62. The method of claim 61, the instructions when executed further operable to create billing reports from the tracked messages.

63. The method of claim 61, the instructions when executed further operable to create call log reports from the tracked messages.

64. The machine-readable medium of claim 60, wherein the networked computerized system resides between a computer data network and a cellular data network.

65. The machine-readable medium of claim 60, wherein the networked computer marks data that has been monitored via the filter rules in the networked computer to indicate monitoring.

66. The machine-readable medium of claim 60, wherein the cellular data traffic comprises multiple data streams encoded via multiple cellular data protocols.

67. The machine-readable medium of claim 60, wherein monitoring cellular data traffic comprises:

intercepting cellular data;

parsing the intercepted data to a data structure that is non-protocol specific; and

comparing the intercepted data in the data structure against filter rules.

68. The method of claim 60, wherein the cellular data comprises mobile equipment cell registration data that is restricted via filter rules to prevent network transmission of the location of cellular mobile equipment.

69. A machine-readable medium with instructions stored thereon, the instructions when executed operable to cause computerized cellular mobile equipment to:

store one or more filter rules, each filter rule corresponding to an undesired data type;

monitor cellular data traffic for data corresponding to one or more of the filter rules; and

restrict processing of the cellular data traffic corresponding to the one or more filter rules.

70. The machine-readable medium of claim 69, wherein the monitoring and restricting occurs in an event monitor, the event monitor operable to limit the function of software executing on the cellular mobile equipment by use of the filter rules.

71. The machine-readable medium of claim 70, wherein limiting the function of software executing on the mobile equipment comprises limiting the ability of executing software to erase or modify data stored on the cellular mobile equipment.

72. The machine-readable medium of claim 69, wherein the filter rules comprise rules that can be configured by a user via operation of the cellular mobile equipment.

73. The machine-readable medium of claim 69, wherein the filter rules comprise rules that are distributed via a server.

74. The machine-readable medium of claim 69, wherein monitoring cellular data traffic comprises:

intercepting cellular data;

parsing the intercepted data to a data structure that is non-protocol specific; and

comparing the intercepted data in the data structure against filter rules.

75. The machine-readable medium of claim 69, wherein restricting processing of data that corresponds to one or more filter rules comprises temporarily halting processing of the data and prompting a cellular system user to determine what action to take.

76. The machine-readable medium of claim 69, wherein restricting processing of data that corresponds to one or more filter rules comprises temporarily halting processing of the data and alerting a user.

77. The machine-readable medium of claim 69, wherein the monitoring and restricting processing of data that corresponds to one or more filter rules occurs in an interface that resides between a subscriber identity module (SIM) and cellular mobile equipment.

78. The machine-readable medium of claim 77, wherein the one or more filter rules restrict modification of data contained in the subscriber identity module (SIM).

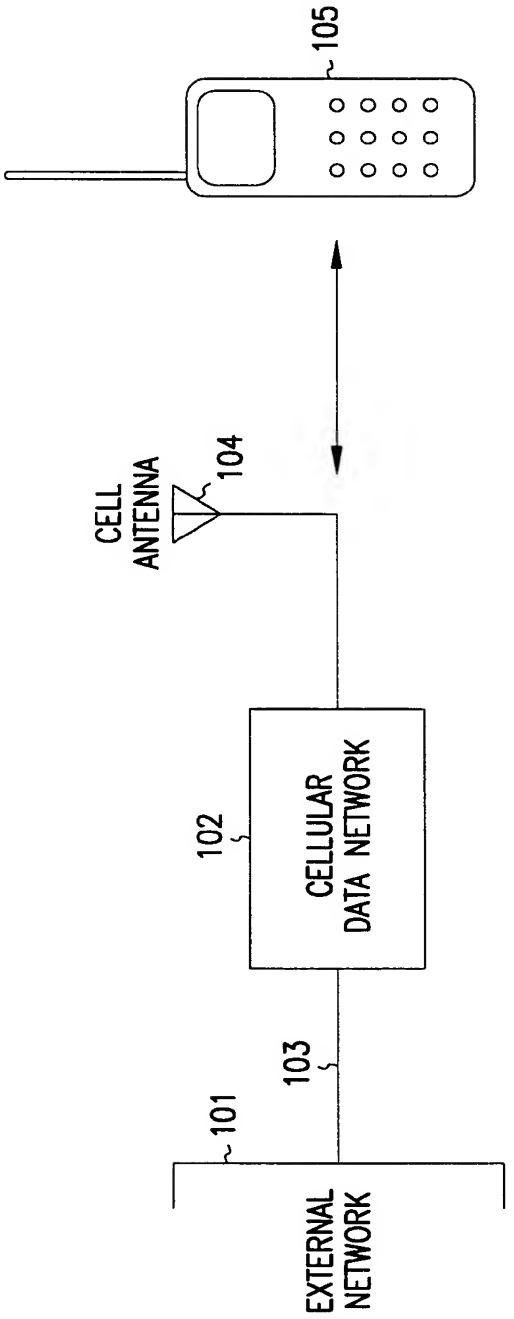

105
CELL ANTENNA
104
102
CELLULAR DATA NETWORK
103
101
EXTERNAL NETWORK

FIG. 1

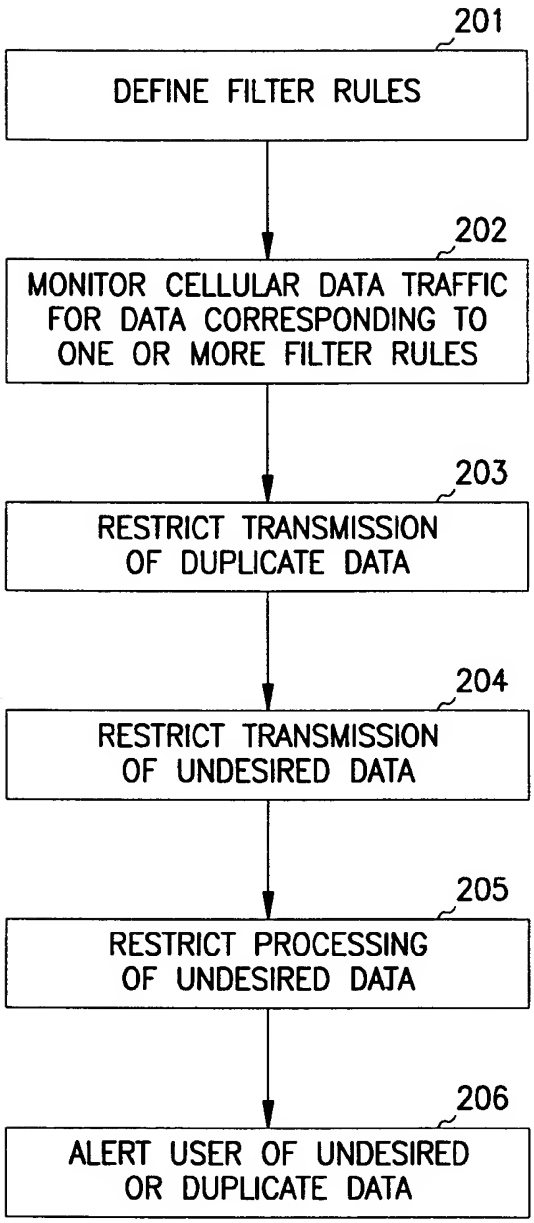

201
DEFINE FILTER RULES
202
MONITOR CELLULAR DATA TRAFFIC FOR DATA CORRESPONDING TO ONE OR MORE FILTER RULES
203
RESTRICT TRANSMISSION OF DUPLICATE DATA
204
RESTRICT TRANSMISSION OF UNDESIRED DATA
205
RESTRICT PROCESSING OF UNDESIRED DATA
206
ALERT USER OF UNDESIRED OR DUPLICATE DATA

FIG. 2

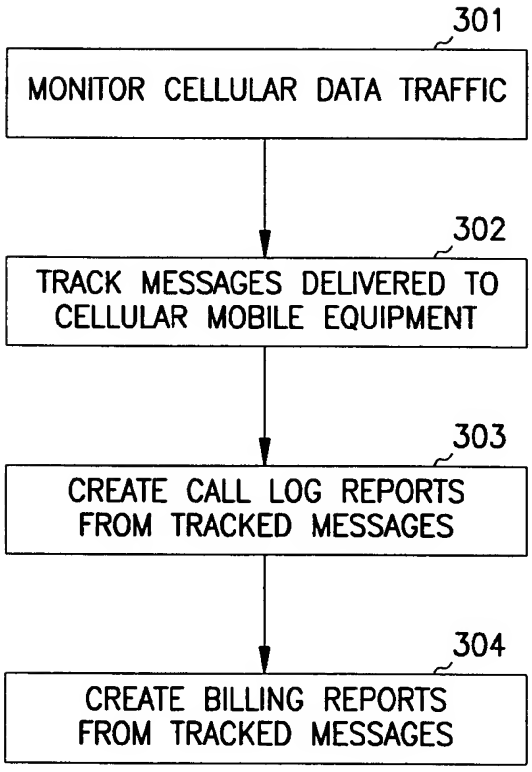

301
MONITOR CELLULAR DATA TRAFFIC
302
TRACK MESSAGES DELIVERED TO CELLULAR MOBILE EQUIPMENT
303
CREATE CALL LOG REPORTS FROM TRACKED MESSAGES
304
CREATE BILLING REPORTS FROM TRACKED MESSAGES

FIG. 3

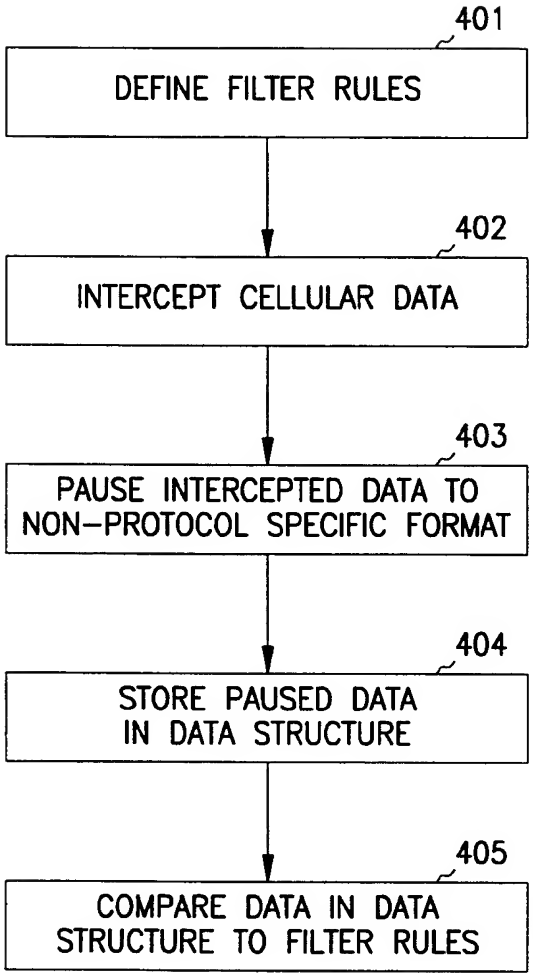

401
DEFINE FILTER RULES
402
INTERCEPT CELLULAR DATA
403
PAUSE INTERCEPTED DATA TO NON-PROTOCOL SPECIFIC FORMAT
404
STORE PAUSED DATA IN DATA STRUCTURE
405
COMPARE DATA IN DATA STRUCTURE TO FILTER RULES

FIG. 4

INTERNATIONAL SEARCH REPORT

Inter ›nal Application No
PCT/IB 00/01586

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98 47270 A (NOKIA TELECOMMUNICATIONS OY ;TUOMINEN JOONAS (FI)) 22 October 1998 (1998-10-22) abstract page 3, line 1 - line 28 page 6, line 22 -page 8, line 25 figure 1 ---	1-78
Y	EP 0 909 073 A (LUCENT TECHNOLOGIES INC) 14 April 1999 (1999-04-14) abstract page 3, line 52 -page 6, line 28 page 7, line 16 - line 32 figures 1-3 --- -/--	1-78

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 February 2001	06/03/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Rabe, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter. nal Application No
PCT/IB 00/01586

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 97 49252 A (MANICKAVASAGAM SENTHILKUMAR ;RADOVIC NIKSA (US); SHAH ASHESH C (US) 24 December 1997 (1997-12-24)	1,7,17, 27,33, 43,53, 54,60,69
A	abstract	2-6, 8-16, 18-26, 28-32, 34-42, 44-52, 55-59, 61-68, 70-78
	page 4, line 21 -page 9, line 31 figure 2	
A	US 5 835 726 A (DOGON GIL ET AL) 10 November 1998 (1998-11-10) abstract column 2, line 66 -column 3, line 29 column 5, line 39 -column 6, line 54 figures 1,2	1-78
A	WO 99 48261 A (SECURE COMPUTING CORP) 23 September 1999 (1999-09-23) abstract page 8, line 23 -page 13, line 12	1-78

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter: nal Application No
PCT/IB 00/01586

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9847270 A	22-10-1998	FI 971615 A	17-10-1998
		AU 6836598 A	11-11-1998
		CN 1256847 T	14-06-2000
		EP 0976270 A	02-02-2000
		ZA 9803145 A	22-10-1998
EP 0909073 A	14-04-1999	US 6098172 A	01-08-2000
		JP 11167537 A	22-06-1999
WO 9749252 A	24-12-1997	AU 3496797 A	07-01-1998
US 5835726 A	10-11-1998	US 5606668 A	25-02-1997
		AU 6135696 A	15-01-1997
		CA 2197548 A	03-01-1997
		EP 0807347 A	19-11-1997
		WO 9700471 A	03-01-1997
		JP 10504168 T	14-04-1998
		NO 970611 A	15-04-1997
		CA 2138058 A	16-06-1995
		DE 69425038 D	03-08-2000
		EP 0658837 A	21-06-1995
		JP 8044642 A	16-02-1996
WO 9948261 A	23-09-1999	EP 1062785 A	27-12-2000